Where's The Beep?

A Case Study of User Misunderstandings of RFID

Jennifer King
School of Information
University of California, Berkeley
Berkeley, CA, USA
jenking@ischool.berkeley.edu

Aylin Selcukoglu
Conifer Research
Chicago, IL, USA
aylin@coniferresearch.com

Abstract—Radio frequency identification (RFID) technology is increasingly being incorporated into everyday objects. This case study examines three examples—credit cards, transit cards, and the U.S. e-Passport—given ubiquitous computing power through the addition of RFID. We explored user comprehension of RFID technology generally and these implementations specifically to understand if and how the addition of this technology transformed subjects' experiences with these objects. By exploring whether or not the new implementations preserved prior expectations of use, we sought to understand what experiences subjects drew upon to create new mental models for engaging with them. As all three of the objects we examine stored personal or financial information, we were specifically interested to understand how individuals dealt with the novel privacy risks introduced by RFID. We distill our findings into general recommendations for designers contemplating embedding ubiquitous computing into everyday objects, particularly those that manage personal or financial information.

Keywords RFID, ubiquitous computing, ubicomp, privacy, mental models, risk, contextual integrity, user expectations.

I. INTRODUCTION

While new innovations often captivate public attention, technological advancements to existing everyday objects can be equally transformative. Yet the changes wrought by the introduction of computational or ubiquitous capabilities into everyday objects requires a critical reexamination by designers of how these objects function, particularly in relation to users' existing expectations.

This case study examines three examples of everyday objects given ubiquitous computing power through the addition of a technological component: radio frequency identification (RFID) chips. The everyday objects we study are credit cards, transit cards (the Bay Area Rapid Transit [BART] EZ-Rider Card or the Clipper (previously TransLink) multi-agency transit card), and the contactless "electronic" U.S. e-Passport. We chose these three objects because in each case the object existed in a pre-RFID form; the object stored data of personal importance to a subject (either personal or financial data) that attached some level of privacy concern; and the object was something a subject would carry with them and use across a variety of contexts and places. We examine how the addition of RFID (in this study, contactless smart card chips) transformed subjects' experiences with these objects. By exploring whether or not the new implementations preserved prior expectations of use, we sought to understand what experiences subjects drew upon to create new mental models for engaging with them. As all three of the objects we examine stored personal or financial information, we were specifically interested to understand how individuals dealt with the novel privacy risks introduced by RFID. We distill our findings into general recommendations for designers contemplating embedding ubiquitous computing into everyday objects, particularly those that manage personal or financial information. We also offer specific recommendations for managing the privacy risks posed by RFID.

A. The Challenges of RFID's Invisible Interface

When embedded into everyday objects, the computational and communicative capacity of RFID is often designed to disappear. Like the objects of our inquiry, RFID chips can be quite small. They usually lack their own power source and are instead powered by the signals emitted from an RFID reader. Consequently they lack both a user interface and a signaling infrastructure, such as speakers or lights, let alone the video display that most technological objects typically use to interact with users. An RFID *reader* may have such capabilities, but most readers are not intended for use by end-users.

This lack of interface presents several challenges for designers incorporating RFID into everyday objects. The new capabilities RFID bestows on an everyday object should be both visible and comprehensible to users. Instead, they often violate users' expectations of how the object is "supposed" to work. Signaling to the user that an action has occurred, or is about to occur, is crucial when the object's behavior diverges from its users' expectations, especially so if a read is not the result of a direct user action. If an implementation does this poorly or not at all, users are left in the dark about what their RFID-enabled objects can and are doing on their behalf. These challenges are further compounded when users are unfamiliar with RFID technology and how it functions. A lack of understanding—as well as a *misunderstanding*—of RFID's capabilities can add to users' confusion and frustration. In instances where product sales are at stake, design flaws like these could annoy users and doom a product's adoption. But RFID is also embedded in artifacts where the public has no alternative options, such as the U.S. e-Passport. In instances

This work was sponsored by TRUST (Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (Award #CCF-0424422).

such as these, a poor implementation could put users' privacy and physical security at risk.

B. Privacy Risks

RFID can be a promiscuous technology: in its most basic implementation, an RFID tag will transmit its stored data to any reader operating at its corresponding frequency. A transmission can occur silently, without any signaling. This promiscuity, coupled with RFID's invisibility and lack of interface, contribute to its potential privacy risks. Because RFID can be deployed in a multitude of ways, assessing the degree of risk requires a case-by-case analysis, dependent on the type of RFID used, the sensitivity of information stored on the chip, whether or not the chip or object offers any security features, and the context in which the implementation is deployed. Many basic implementations offer no security features, making tracking via the chip's static identifier the most common risk, especially when the object is deployed in public places.

While there have been efforts to address both security and privacy issues at the chip design level [7,9,16], these efforts have yet to gain wide acceptance, and thus users often bear some or all of the burden of mitigating privacy threats. For example, the original proposal for the U.S. e-Passport had no security features in place to protect the passport holder's personal data, and the Department of State, in response to public criticism, incorporated both a foil shield into the cover to prevent unauthorized reads, as well as chip encryption (Basic Access Control), into the final e-Passport design [10]. Heydt-Benjamin et al. [3] discovered in 2006 that credit card issuers were not encrypting the data stored on RFID-enabled credit cards (i.e., cardholder name, card number, and expiration date), and as of 2010 this remained the case, though some issuers have since replaced the cardholder name field with a generic placeholder (e.g., "Valued Cardholder"). This lack of security is only viable as long as compliant readers or software are not obtained or hacked by malicious parties.

The RFID-enabled objects we examine in this case study use contactless smart card technology, embedded with a passive RFID chip operating at 13.56Mhz with a recommended read range, per the ISO 14443 standard, of four to six inches. Of these objects, only the transit card and the e-Passport use smart cards' authentication and cryptographic abilities.

C. Contextual Integrity: A Theoretical Framework for Harmonizing New Information Flows with Privacy Norms

The new capabilities of the objects we study here require users to learn new modes of interaction. For example, in the original form factors an explicit act was required to share information, such as swiping a credit card through a magnetic stripe reader, or feeding a transit ticket into a ticket machine. With the addition of RFID, the same information can be transferred without any direct action on the part of the user and without the card coming into direct physical contact with a reader or an individual. These new capabilities force users to relearn how these objects "work." To do so, users draw upon expectations set by their experience with using the object in its previous state. But even if the object serves the same overall purpose, the addition of RFID can violate the established expectations based on prior use of the object. More importantly for our inquiry, the shift in the objects' actions in the world may violate the existing norms, or social rules, of information flow that were previously reflected in the object. For example, asking users to learn to "tap" or hover an RFID credit card over a reader instead of physically swiping it through one represents change in interaction. But an adversary standing next to a user reading a RFID credit card through her bag without her knowledge is a violation of the norms of information flow for the object.

Philosopher Helen Nissenbaum posits that all environments are governed by norms of information flow and that privacy violations occur when these norms are breached [14]. In particular, she highlights that respect or consistency with norms of appropriateness and distribution in a given context are key to protecting privacy. Her theory of privacy, "Contextual Integrity," [13] provides a useful descriptive framework for analyzing the potential of new technologies to disrupt information privacy. By documenting the norms that govern information flows prior to the introduction of a new technology, and exploring where the new technology will change the data collected (appropriateness) and the means and entities to whom it is distributed (distribution), Contextual Integrity assists in identifying information practices at odds with extant contextual privacy norms.

Nissenbaum uses an example of RFID tags to illustrate violations of contextual integrity, noting that RFID can "significantly alter the nature and distribution patterns of information." Discussing RFID specifically in the context of item-level tagging of consumer products, something that is just now becoming a reality in the U.S. [1], she notes that unless implementations of RFID allow for easy detection and disabling of the tags, "discretion is removed from the consumer and placed into the hands of information gatherers". We argue here that because RFID can transmit information without any direct action by users, users without a basic understanding of how RFID functions risk privacy violations. Unless they are actively informed of the new information flows RFID enables, users will not be able to modify their use of RFID-enabled objects or otherwise force the objects to respect contextual privacy norms. This is especially true in cases where the implementation introduces new information flows, changes how information is disclosed, or introduces new agents to the transaction.

II. Related Work

To date, there are few studies that investigate general user comprehension and interaction with RFID. Many user studies are focused on novel uses or prototypes, and are often restricted to laboratory environments. Three studies are most relevant to our work. Mäkelä et al. [8] conducted a field study that examined subject interactions with RFID tags compared to 2D barcodes, using mobile phones as readers for both. The authors noted the novelty of this paradigm, and reported "potential usability risks," as subject mental models, lacking much relevant prior experience to draw from for comparison, were vague.

Poole et al. [15] explored subject perceptions of RFID by examining public perceptions and folk theories about the technology in order to discuss the influence of non-functional criteria (i.e., associations of ethics, value judgments, social appropriateness, and comprehension of internal workings) generally on the development, adoption, success, and failure of ubiquitous technologies. The researchers conducted semi-structured interviews and a photo-elicitation exercise with thirty-five subjects; each was shown a set of photos, some with a direct association to RFID. Subjects were prompted to discuss whether or not they thought the photo was associated with RFID and why. The subjects showed "significant confusion about what RFID is and how it functions," often conflating its capabilities with global positioning systems (incorrectly believing it provided long range tracking capabilities), or that it functioned similarly to magnetic strips and optically scannable bar codes. Over two-thirds of subjects had direct experience with RFID through pet ID chips and transit cards, but even so these subjects were uncertain about RFID's capabilities. In sum, they reasoned that incorrect models can "make people uncomfortable in adopting or using the technology, even in cases where such fears may be unwarranted." At the same time, they note that legitimate concerns about trust and accuracy are difficult or impossible to address when the inner workings of the system are unintelligible—or in RFID's case, "effectively invisible."

Lastly, Nguyen et al. [12] conducted a user study exploring attitudes and concerns about everyday tracking and recording technologies, including RFID. However, this work did not attempt to ascertain what people understood about the technology (in fact, a key component of the study involved educating subjects about how RFID worked prior to asking them questions about their attitudes towards RFID as a tracking technology), though they mention as a side-effect of their interview process that subjects had "flawed mental models of the inner workings of technologies, which contributed to their difficulty in understanding the potential threats." Subjects were asked about their level of concern about strangers, government, thieves, and companies tracking RFID tagged goods or personal items; subjects demonstrated a high level of concern across all entities, though when asked to weigh the potential advantages versus disadvantages, "the majority of subjects reported favoring the potential advantages." The study does not include the educational materials or a discussion of what benefits and disadvantages were articulated to subjects, thus is it unclear what positives and negatives the subjects were asked to evaluate and what impact this may have had on their answers.

III. METHODS

Our study consisted of two phases: an exploratory study with nine subjects, where we tested our approach, and a final study with twenty-eight subjects consisting of a short survey instrument, an image evaluation exercise, and an hour long semi-structured interview.

Our primary goal was to examine user comprehension of RFID and how it influenced their relationship to each object. We asked: what are subjects' mental models of how RFID systems work, and how do they compare to the actual functioning of these systems? Secondarily, we evaluated each object's compliance with contextual integrity (i.e., did the new implementation conform to existing norms of appropriateness and information flow). We also explored the impact of subjects' comprehension of RFID on their ability to perceive any privacy risks presented by the new implementation. Did subjects understand that tags or chips can be read without their knowledge? How did their mental models combined with their knowledge (or lack thereof) of RFID affect their ability to make risk assessments about potential privacy threats, both generally and with reference to their specific objects?

A. *Preliminary Study: Refining Mental Models*

Following an approach outlined by Morgan et al. [11], we chose to conduct a series of exploratory qualitative interviews, structured to elicit subjects' mental models of radio-based communication generally, and of existing implementations of RFID technology specifically. We recruited nine subjects through word of mouth at our university to meet distinct cases outlined by two three-state criteria: general technical familiarity (novice, intermediate, advanced) and possession of particular RFID objects (transit card, credit card, and the e-Passport).[6] Based on this preliminary work, we made refinements to our survey and interview protocol and added an image evaluation component to our final study.

The analysis of mental models is well established in usability research, and is appropriate for ascertaining users' understanding of their tools and those tools' vulnerabilities. Building on theory developed by Craik [2], Johnson-Laird argues in [4] and [5] that mental models are a central feature of cognition and comprehension. Donald Norman has famously applied this theory to system design and usability, describing the critical features of useful models [14], in addition to advocating comparison of users' models to expert models of systems. Morgan et al. [11] has applied mental models to the study of risk communications in an effort to create "public-centered" risk information, a concept applicable to privacy risks. With respect to RFID specifically, [8] and [14] have used a mental models approach to explore user comprehension.

As Norman [14] and others have cautioned about difficulties with the elicitation of mental models, we pre-tested several inductive approaches. Rather than immediately asking subjects to describe the workings of the devices they had used, we focused on use cases, inferring and eliciting subjects' assumptions and mental models based on their described actions. Subjects were also encouraged to draw comparisons to other technologies, in the hopes that those comparisons would further uncover their understanding of their RFID-enabled objects. We did not assume that subjects had any prior knowledge of RFID, but did require that each owned least one of the examined objects.

B. *Final Study*

Twenty-eight subjects were recruited for the final study: ten credit card users, twelve e-Passport holders, and six transit card users. Subjects ranged in age from 18-64, with forty percent of the subjects between the ages of 25-34, and an even split between males and females and a mix of ethnicities. The youngest subject had just completed high-school; the remainder

of the pool had at least some college education, and twenty five percent had a graduate degree. Subjects were recruited through a local Craigslist ad advertising a one-hour general technology study and were asked to fill out a brief screening evaluation prior to being invited to participate. All subjects were required to bring their object with them to the interview, and received a $25 gift card upon completion. Subjects completed a short baseline survey regarding their use of and familiarity with various wireless technologies as well as with RFID. Sixteen subjects (57 percent) had not heard of RFID before, and twenty-two (79 percent) professed little or no understanding of RFID. Five subjects claimed a moderate understanding, and only one subject claimed to have an advanced understanding of RFID.

1) Study Procedures

A subject's survey responses served as the starting point for a semi-structured interview in which the subject described when and how he/she used a particular object. Reviewing the subject's answers about familiar wireless technologies (such as garage door openers) with them proved useful in eliciting subjects' perceptions of RFID. We encouraged subjects to verbalize the thought processes they used to answer the survey questions and explored their answers in more detail with follow-up questioning.

The interview protocol was designed to probe the rationale and comprehension underlying the subjects' use of their RFID-enabled objects, as well as to uncover their perceptions of the benefits and drawbacks. We developed three protocols that shared the same overall structure and emphases but included questions specific to each individual object. After completion of the interview portion, subjects were given an image exercise where they were asked to select the image that best represented their understanding of how their object interacted with an RFID reader. Subjects were next shown communication materials produced by the issuer of their object (i.e., a pamphlet, webpage, or online video providing an overview of how to use the object) and then asked to explain if the material aided their understanding of the object's operation in any way, communicated any advantages, or helped them understand any differences with the new implementation or potential risks.

Finally, subjects were shown a functional RFID reader and asked to demonstrate how they thought it worked with their object. Results from this portion of the study varied widely since all transit card users had used their cards with a reader, most of the credit card users had, but none of the e-Passport holders had since, at the time the study was conducted, the U.S. was not yet using e-Passport readers at ports of entry. At the conclusion of the interview, subjects were debriefed about RFID and the security measures in place for their objects. All interviews were recorded with the subjects' permission and transcripts were made for coding purposes.

IV. FINDINGS

In this section, we review the findings from each phase of the study, discussing both overall findings as well as issues specific to each object.

A. Survey Results

We reviewed aloud with subjects their self-reported familiarity level with a list of wireless products (i.e., garage door openers, television remotes, keyless car remotes, keyless door badges, toll transponders, wireless internet, mobile phones, GPS units, and pet ID chips) in order to frame the discussion around related technologies without revealing that the topic of the study was RFID. We did not want to influence subjects' opinions about RFID by providing a definition that skewed further discussion. For each product, we asked the subject whether or not they had used it before and what they felt their level of understanding of how it "worked" was. As we reviewed their answers, we asked subjects to verbalize the rationale behind what they chose and asked if they had ever experienced any problems using the product in order to probe how well subjects understood radio frequency (e.g., if their computer's wireless connection gave them problems and how they tried to rectify it, in order to ascertain if they understood the radio transmission component). A few subjects had a clear understanding of how radio frequency differed from, for example, infrared-based remotes:

***P9**: I noticed opening your car you can do it from ways away and the direction doesn't matter there's no—it's not an infrared beam so there's no area you need to aim it . . . it's broadcasting in all directions, all at once.*

While many subjects had a basic understanding of how radio-based products communicate and were aware that radio frequency products could have difficulties transmitting, almost none had a systematic understanding as to what factors could affect this. And understanding the basics of radio frequency did not necessarily mean subjects understood how RFID worked. Five subjects demonstrated a flawed understanding of RFID, likening it to global positioning satellites (GPS). For example:

***P15**: Well, I thought that it worked by satellite so that the chip somehow has a signal, sort of like a GPS. I can't imagine how else it could cover an area like a city.*

The survey next asked subjects about their comfort level with four RFID-based scenarios: using a contactless device to gain entry to their home, traveling with a prepaid contactless transit card, making a purchase with a contactless credit card, and traveling with an e-Passport. Results are summarized in Table 1. Most subjects were able to ascertain what was meant by contactless, though a few thought the term meant "anonymous," i.e., requiring no contact information. The context of use was important for predicting acceptance; subjects reported the least comfort with using a keyless entry to their home and the most comfort with using transit cards. Specifically, several respondents noted that the concept of using a keyless entry felt less secure than a physical key:

***P6**: I think in a way it almost would be easier, with how much advances in technology there are currently, to change or manipulate a frequency opposed to picking a lock.*

We also asked subjects directly about RFID in the survey: had they heard the term before; to the best of their knowledge if they owned any products that contained RFID; how they rated their understanding of how it functioned; and their general impressions about it. Results are summarized in Table 2;

overall, our subject pool was unfamiliar with RFID and had a neutral disposition toward the technology.

TABLE I. COMFORT LEVELS WITH HYPOTHETICAL SCENARIOS ON A 5 POINT LIKERT SCALE. *HIGHER VALUES INDICATE MORE COMFORT.*

Q: Please rate your comfort level with the following scenarios:	**Mean (SD)**
Using a keyless/contactless device to gain access to your home	3.39 (1.29)
Traveling with a contactless/electronic passport (the new "e-Passport")	3.52 (1.44)
Making a purchase using a contactless credit card	3.58 (1.24)
Traveling with a prepaid contactless transit pass	4.30 (1.10)

TABLE II. GENERAL IMPRESSIONS OF RFID

		Yes	**No**
Have you heard of the term RFID before?		57%	43%
	Yes	**No**	**Don't know**
To the best of your knowledge, do you own any products that contain RFID?	14%	21%	64%
	Little/ None	**Mod.**	**Adv.**
Please rate your personal understanding of RFID	79%	18%	4%
			Mean (SD)
What is your general impression of RFID? (5 point Likert scale, higher value = more positive impression)			3.14 (.651)

During the interview, subjects were asked to complete an exercise where they selected the image that best matched their understanding of how their object communicated with a reader. Subjects were shown four incorrect images and one correct image. The images were identical for all three objects; only the object name was changed to match what the subject owned.

Only eight (30 percent) of our twenty-eight subjects chose the correct answer, an image illustrating the omni-directionality of radio frequency signals with a caption noting that the reader initiates communication to the object. The most popular (yet incorrect) choice portrayed a reader and the subjects' RFID object sensing the other's presence simultaneously and communicating in a directional manner. Eleven (41 percent) of our subjects chose it as the correct answer.

B. Interview Results

In this section, we will first discuss common findings across all three objects, and then specific findings for individual objects in turn.

1) Commonalities

Common themes in subjects' perceptions of the benefits of RFID for all three objects were speed and convenience. Even with the e-Passport, which no one had used the RFID component, subjects assumed the inclusion of RFID would make border crossings faster. Physical wear of the non-RFID objects (malfunctioning paper transit tickets, demagnetizing credit cards), a dislike of dealing with cash, and the ease of tracking electronic payments were mentioned frequently as benefits of the contactless versions.

Like the hypothetical scenarios we asked subjects about in our survey, the context of use was key for predicting general comfort with the three implementations. Subjects were most comfortable with the use of RFID in transit cards both because their transit travel history did not seem particularly sensitive to them (though there was a general expectation that the information was secured), and because the transit cards in this study were limited in their financial scope: stored value cards that had a maximum value (i.e., the cards would recharge at a certain point but were not tied directly to a checking or savings account).

P13*: Getting a bus pass, yeah, great—who's going to try and crack it? You know what I mean? It's kind of, like, there's not a lot of benefit to [the hacker].*

P6*: I probably wouldn't be putting large sums of money on a transit pass. And if I did lose it, it wouldn't be the end of the world.*

Several subjects mentioned they liked the limited use, single functionality transit cards, though others professed interest in a unified device, some mentioning the use of mobile phones in Japan used as payment devices (though a few noted that losing that type of mobile phone would be extremely problematic).

While there was universal acceptance and comfort with RFID-enabled transit cards, credit cards and the e-Passport were more problematic. Subjects perceived little benefit with the addition of RFID to either object, and the fact that they could be read from a distance coupled with the sensitivity of data believed to be stored on each led subjects to be distrustful of the feature.

There was a universal expectation with all of the objects that an RFID reader would provide a visible or audible signal when reading.

P21*: I would expect a light to change or there would be a sound. There would be something that would indicate—there would be feedback that would say if it had been read or not.*

Most subjects also expected that all of the objects would only be readable from a short range. They were generally unaware that some RFID chips could be read from distances greater than a few inches, or that chips could be read without visual or audio feedback, or for that matter, without their consent or knowledge. Subjects were generally uncertain of whether or not any security measures were in place for the objects we examined, though many expected that there must be.

When attempting to explain how RFID worked, nearly every subject made comparisons to optical scan technologies with similar use cases, usually bar codes, with the expectation that a chip had to be in visual line-of-sight proximity to a reader. This finding clarifies why during the image exercise 65 percent of our subjects chose an image that illustrated a

directional, line-of-sight communication between chip and reader.

***P6**: I would assume that there is some type of like mechanism within that machine that is shooting some type of frequency or some type of light sensor, and that it's hitting the barcode or hitting some kind of decal or sensor on a product. Some form of light or radio or other type of frequency that I'm not knowledgeable about.*

This notion is contradictory to the omni-directional way in which RFID signals are broadcast, a subtle distinction with significant implications for design. And each object's documentation wasn't helpful in clarifying this: in reviewing online (and offline, when available) documentation and marketing materials for each of these objects, none discussed any security measures or any potential risk with the exception of the e-Passport. In the case of the e-Passport, the attempt at risk communication was poorly made; upon review of an official e-Passport brochure describing the passport's security features, subjects were generally unable to ascertain what risks were present or what security measures were in place. This led to some skepticism around how secure their data was:

***P6**: But I think a lot of times protection is promised when it's actually just exposing [you].*

Subjects were usually unaware of what data was stored on each object, sometimes assuming far more (such as social security numbers and home addresses on the credit card, or travel histories and security clearances on the passport) than was actually present. Again, this was understandable, since the vendors did not publish this information in their public communications materials. At the same time, many subjects noted that while better information could be helpful, many didn't care how their devices worked—they just wanted them to work and didn't want to invest time in learning more about the technology.

2) Credit Cards

Our ten credit card users had either Visa PayWave or MasterCard PayPass cards, and nine of the subjects were not aware the cards contained RFID. Five had used the RFID feature prior to the study, and five had not. The benefits voiced most often were convenience and time savings. However, several expressed skepticism over what benefit adding RFID to the credit card gave them since most merchants offer terminals that already allow you to swipe the magnetic stripe card yourself, and the contactless feature didn't seem to offer a substantial time savings.

***P13**: I don't really know too much about this other than you just tap it and actually, quite frankly, probably the only benefit to me to this is maybe sometimes you don't have to keep doing that. That's the only kind of thing I see about it. I look at it more as a marketing gimmick than anything else.*

The primary concerns expressed were the possibility of malfunction, typically with erroneous charges and over-deductions, and no longer signing for purchases, which is an option for both RFID and non-RFID credit cards at some merchants for purchases $25 or under.

***P4**: Because what if it just accidentally takes too much money? How would I know [without a receipt]? And then you find out after the fact—how would you fix that?*

Not requiring a signature was an interesting change of context because no one was certain what the consequences of signing a receipt actually were—most just felt more secure doing it. One subject conjectured:

***P20**: [Not signing] kind of worries me a little bit, because if my card gets stolen, then there's no real way to verify that someone is the right owner. But if it came down to it, maybe if you went to the bank and there's a bunch of records not with your signature on it, maybe you could get money back. [I'm] not exactly positive how it works.*

Regardless, this change of context made some subjects uncomfortable. At the same time, several subjects noted that they routinely checked their statements online or on paper, and thus they felt they would be able to detect if erroneous charges appeared.

We asked subjects to demonstrate using their credit card to pay for an item with our reader. Half of the credit card users said the read range was what they expected (the other half thought it would be longer than four to six inches). Several were explicitly concerned with the card's contactless capabilities because of way such an implementation could expose their credit card number (a sensitive piece of information) and the financial hassles theft could cause.

***P2**: At least with a credit card, I know it's in my wallet, it's kind of safe. I have to actually take it out and use it. So that is why the [contactless] option makes me a little nervous.*

3) U.S. e-Passport

Twelve of our subjects were e-Passport holders; four knew the passport contained RFID, and eight did not. When traveling, subjects most commonly carried their passports physically on them at all times. In addition to traveling, subjects mentioned many situations where they used their passports for identification; for some, it was their primary form of ID. The only personal benefit mentioned by subjects was the assumption that RFID would make border crossings speedier; most assumed RFID was introduced into the passport for the benefit of the government, typically to make it more difficult to counterfeit, or to fight terrorism.

Subjects' concerns mainly focused on whether or not the chip enabled the government to more easily track their whereabouts when traveling. Seven subjects in fact believed the e-Passport did allow this.

***P4**: I feel almost like there must be a chip in here somewhere and they're tracking me, you know, like the FasTrak (toll tag) only where you're going and what time you're going through. I think they're probably just tracking where you're going, but I don't know.*

Fears of malfunction were often voiced; many subjects assumed that the embedded chip needed to be functional in order for their passports to be valid (which it does not).

***P10**: I wouldn't want to be stranded somewhere just because this was faulty or didn't work.*

More than the other two objects we studied, subjects not only saw little direct benefit to them with the addition of RFID, they also were unaware of its purpose. This is understandable, considering that the inclusion of RFID was not for their direct benefit. At the same time, our subjects had definite expectations of what they thought it could and should do, grounded in their experiences traveling with older passports or with their new one, though none had, to the best of their knowledge, seen their passports read using the chip at a port of entry. For example, none imagined that the inclusion of RFID could allow their passport data to be read without their knowledge. We should note that based on the final design of the e-Passport, this is difficult to do; the cover of the passport contains a metallic foil that prevents the chip from being queried unless it is open .25 inches or more. In addition, the chip's security layer requires a "pin code" in order to read its contents; without the pin, the chip can be queried, but it only returns a rotating numeric identifier. However, as mentioned previously, the original design lacked these security features; it was only after substantial negative public feedback that the design changed to one more clearly aligned with user expectations.

As it happens, the normal wear and tear passports endure often leaves their covers open past the required quarter-inch to allow the chip to be queried. We saw this in the passports we examined: the bindings were relaxed on those that had been opened frequently, and we could often query the chip with the passport sitting atop of our reader with the cover "closed" as it would no longer close completely without assistance (e.g., by looping a rubber band around it). And our subjects reported a variety of abuses—stuffing travel documents inside them, squeezing them into money belts, strapping one to one's leg in the South American jungle—that rendered the protective powers of the metallic cover useless unless it was forcibly held closed (a feature none of our subjects was aware of). After having been shown how a passport is read, all subjects admitted that if someone read it without their consent, they would be unaware it happened.

4) Transit Cards

Six of our subjects were transit card users, and several of our other subjects also used transit cards, mentioning them for comparison throughout their interviews. Three subjects knew their card contained RFID, and three did not. Subjects listed many benefits with transit cards: convenience, ease of use, auto-replenishment, elimination of paper tickets (which are notoriously unreliable on BART), a sturdy and reliable form factor, and a general dislike of using cash for transit (e.g., needing exact change).

***P3**: The reason I got this was because the [tickets] kept getting demagnetized so from a utilitarian standpoint it was just annoying—don't put it next to your cell phone. How many people don't do this? That was really frustrating.*

Few concerns were voiced about transit cards. More than e-Passports and credit cards, subjects felt it was an appropriate use of the technology, both as a physical stand-in for the tickets and passes it replaced and for the data it managed. There was a universal expectation of feedback—at least a beep and a light flash—but also for the systems to signal acceptance (e.g., an open gate) or rejection (e.g., a red light or "sad" beep), and to show the remaining card balance.

***P12**: It beeps. It makes a nice beepy sound. And then [the transit card] shows you your balance on the display. It says "Tag your card" on it. So I shoved the card against it. I was afraid it wasn't going to work at first so I avoided using it for the first couple of weeks, but after I started using it, it was really self-explanatory.*

V. DISCUSSION

The majority of our subjects did not understand how RFID functioned. Similar to the findings by Poole [15], our subjects most often expected it to function like optical scan technologies, assuming the chip must be in visual line-of-sight proximity to a reader. This finding can be attributed to the fact that RFID often acts like a bar code (even if users don't understand that it is enabling far more sophisticated item-level tracking) and the interaction most have had with RFID readers is quite similar to that of using an optical scanner. There was a near universal expectation of signaling—a beep or a light flash—when an object was being read. It surprised us that demonstrating at least a surface understanding of how radio-based objects communicated did not mean our subjects had any better insight into how RFID worked. Instead, the similarity of the interaction to optical scan or magnetic stripe readers, in the absence of any visibility into the RFID component, held far greater sway over subjects' mental models. Clearly, designers must keep in mind that references to similar technologies may dominate users' mental models, and that specific efforts may be required to educate users how RFID has changed an existing object's capabilities and information flow.

Designers should keep in mind that when introducing ubiquitous technology to everyday objects, recognition of new abilities, when applicable, is also crucial for users to take steps to mitigate risks. This is particularly important with RFID since physical shielding is required to block radio frequency transmissions. Most of our subjects had not encountered any communications about these new capabilities (e.g., that their objects could be read from distances greater than a few inches, without producing any visual or audio feedback, or without their knowledge or consent) which left them unaware and exposed to the risk of information on their object being read by an unauthorized party or when they didn't expect it to be – a violation of their expected information flows.

Even though most of our subjects were not interested in the in-depth inner workings of their objects, since they lacked important information (e.g., what data was stored on each object, that RFID signals are broadcast in an omni-directional way, what security features were present) to help them knowledgably assess the risk they faced by using the object as well as their comfort level with this risk. Rather than placing the burden on users, designers should create implementations that mitigate or eliminate these risks. If that isn't possible, then they should share the responsibility of protecting user privacy by creating targeted communication and documentation around these issues to alleviate uncertainty.

Subjects were uncomfortable with cases where RFID extended objects' capabilities in ways that did not directly

benefit them or violated their contextual integrity. The level of discomfort was a function of how sensitive the information involved was; transit cards and credit cards both involve money, but transit cards were considered far more acceptable given the relative insensitivity of travel data, the cards' limited financial value, the restrictiveness of use (in this case, only on the transit system itself), and how congruent their contactless features were with their previous form factor.

In contrast to Poole's [15] findings, overall our subjects demonstrated trust in the designers of these products—specifically, that despite the introduction RFID, the information these objects stored and communicated would be protected, even if our subjects didn't understand how it worked. This expectation was rooted in subjects' experience with the non-RFID versions, where the information stored on these objects could not be copied or tampered with without physically taking the object away from its owner. Subjects trusted that the addition of RFID wouldn't change the data's information flow. This trust offers a cautionary tale to others considering extending the functionality of existing objects with RFID—users will expect the contextual integrity of the information flows to remain the same despite changes in the form factor. Designers betray that trust at their peril.

To maintain the integrity of information flows and protect individual privacy, designers should ensure that their implementation does not allow the chip to be queried without the user's knowledge and consent and does not allow a third party to track or infer information about the user (e.g., a static identifier that could be associated with that user) through data broadcast by the chip. They should consider incorporating a physical shield or adopting designs like those proposed in [9] to prevent all radio frequency communication without explicit consent of the user.

VI. CONCLUSION

This case study examined three examples of everyday objects—credit cards, transit cards, and the U.S. e-Passport—given ubiquitous computing power through the addition of RFID chips. We found that subjects were uncomfortable with instances where RFID extended objects' capabilities in ways that did not directly benefit them or violated their contextual integrity. Subjects trusted that the information these objects stored and communicated would be protected, even if they didn't understand how they worked, and the majority didn't; subjects lacked a mental model of how RFID functions, comparing it to line-of-sight, optical scan technologies. This lack of understanding combined with the trust subjects put in the designers of such objects left them unfairly exposed—unable to knowledgeably assess or properly mitigate risks posed by the addition of RFID to their objects. Better consumer and end user communication, coupled with secure, contextually appropriate implementations of RFID that do not leave end users asking "where's the beep?" will pave the way for more widespread acceptance of the technology.

VII. ACKNOWLEDGMENT

The authors wish to thank Andrew McDiarmid for his significant contributions to the preliminary study, and Liz Goodman, Coye Cheshire, and Deirdre Mulligan for their valuable feedback.

VIII. REFERENCES

[1] Bustillo, Miguel. "Wal-Mart Radio Tags to Track Clothing." The Wall Street Journal, July 23, 2010. Available at: http://online.wsj.com/article/SB10001424052748704421304575383213061198090.html. Last accessed October 8, 2010.

[2] Craik, Kenneth J.W., The Nature of Explanation, Cambridge and New York: Cambridge University Press and The MacMillan Co., 1943.

[3] Heydt-Benjamin, T.S., Bailey, D.V., Fu, K., Juels, A., O'Hare, T. Vulnerabilities in First-Generation RFID-Enabled Credit Cards. In Proceedings of Eleventh International Conference on Financial Cryptography and Data Security, Lowlands, Scarborough, Trinidad/Tobago, February 2007.

[4] Johnson-Laird, P.N. Mental Models. In Posner, M. I., ed. The Foundations of Cognitive Science. Cambridge, MA: MIT Press, 1989. 469-499.

[5] Johnson-Laird, P. N. Mental Models: Toward a Cognitive Science of Language, Inference, and Consciousness. Cambridge, MA: Harvard University Press, 1983.

[6] King, Jennifer and McDiarmid, Andrew. 2008. Where's the beep?: security, privacy, and user misunderstandings of RFID. In *Proceedings of the 1st Conference on Usability, Psychology, and Security* (UPSEC'08), Elizabeth Churchill and Rachna Dhamija (Eds.). USENIX Association, Berkeley, CA, USA, , Article 3 , 8 pages.

[7] Langheinrich, M. Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems. Ubicomp 2001. Springer, Atlanta, GA, USA (2001) 273-291.

[8] Mäkelä, K., Belt, S., Greenblatt D., Häkkilä, J. Mobile Interaction with Visual and RFID Tags – A Field Study on User Perceptions. CHI 2007. Available at: http://doi.acm.org/10.1145/1240624.1240774

[9] Marquardt, N., Taylor, A., Villar, N., and Greenberg, S. Rethinking RFID: Awareness and Control for Interaction with RFID Systems. CHI 2010. Available at: http://doi.acm.org/10.1145/1753326.1753674.

[10] Meingast, M., King, J., Mulligan, D. Embedded RFID and Everyday Things: A Case Study of the Security and Privacy Risks of the U.S. e-Passport. In Proceedings of IEEE International Conference on RFID, 2007, 7-14.

[11] Morgan, M.G., Fischoff, B., Bostrom, A., Atman, C. Risk Communication: A Mental Models Approach. Cambridge, UK: The Cambridge University Press, 2002.

[12] Nguyen, D. H., Kobsa, A., and Hayes, G. R. 2008. An empirical investigation of concerns of everyday tracking and recording technologies. In Proceedings of the 10th international Conference on Ubiquitous Computing (Seoul, Korea, September 21 - 24, 2008). UbiComp '08, vol. 344. ACM, New York, NY, 182-191. Available at: http://doi.acm.org/10.1145/1409635.1409661

[13] Nissenbaum, H. Privacy as Contextual Integrity. Washington Law Review Vol. 79, No. 1, February 2004: 119-157.

[14] Nissenbaum, H. Privacy In Context: Technology, Policy, and the Integrity of Social Life. Stanford, CA: Stanford University Press. 2010.

[15] Norman, D. Some Observations on Mental Models. In Gentner, D., and Stevens, L., eds. Mental Models Hillsdale, NJ: L. Erlbaum Associates, 1983. 7-14.

[16] Poole, E. S., Le Dantec, C. A., Eagan, J. R., and Edwards, W. K. 2008. Reflecting on the invisible: understanding end-user perceptions of ubiquitous computing. In Proceedings of the 10th international Conference on Ubiquitous Computing (Seoul, Korea, September 21 - 24, 2008). UbiComp '08, vol. 344. ACM, New York, NY, 192-201. DOI= http://doi.acm.org/10.1145/1409635.1409662

[17] Sullivan, L. IBM RFID Tag May Ease Privacy Concerns. Information Week, May 2, 2006. http://www.informationweek.com/news/mobility/RFID/showArticle.jhtml?articleID=187002857. Last accessed October 8, 2010.